WHAT IS CLAIMED IS:

1. A method of enhancing the security of a message sent by a principal from a client computer through a network server to a destination server, comprising the steps of:

(a) obtaining by the client computer credentials for authorizing the principal from a validation center;

(b) establishing a secure connection for exchanging data between the client and the network server;

(c) transmitting from the client computer to the network server the principal-authenticating credentials and the message;

(d) transmitting the principal-authenticating credentials from the network server to the validation center;

(e) transmitting permission data for the network server from the validation center to the network server based on the principal-authenticating credentials;

(f) verifying the authorization of the principal in the network server to access a digital certificate and issuing a digital certificate to the network server;

(g) establishing a secure connection for exchanging data between the network server and the destination server based on the digital certificate; and

(h) transmitting the message to the destination server.

2. The method of claim 1, wherein the establishing step (a) utilizes the Secure Sockets Layer (SSL) protocol.

3. The method of claim 1, wherein the establishing step (a) further comprises the substeps of:

transmitting from the network server to the client server a network server key associated with a public-private key pair and a known cryptographic algorithm;

transmitting from the client server to the network server a session key encrypted using the known cryptographic algorithm and the network server key; and

transmitting from the network server to the client server information encrypted using the known cryptographic algorithm and the session key to authenticate the network server to the client server.

4. The method of claim 1, wherein the establishing step (g) utilizes the Secure Sockets Layer (SSL) protocol.

5. The method of claim 1, wherein the establishing step (g) further comprises the substeps of:

transmitting from the destination server to the network server a destination server key associated with a public-private key pair and a known cryptographic algorithm;

transmitting from the network server to the destination server a session key encrypted using the known cryptographic algorithm and the destination server key; and

transmitting from the destination server to the network server information encrypted using the known cryptographic algorithm and the session key to authenticate the destination server to the network server.

6. The method of claim 1, wherein the obtaining step (b) further comprises the substeps of:

sending a request for credentials for the principal to the validating center;

receiving the credentials for the principal for from the validation center; and

storing the credentials in the credentials cache on the client server.

7. The method of claim 1 wherein the principal-authenticating credentials comprise a ticket-granting ticket and a session key.

8. The method of claim 7 wherein the transmitting step (d) further comprises the substep of:

transmitting from the network server to the validating center a ticket-granting ticket and an authenticator.

9. The method of claim 8 wherein the ticket-granting ticket comprises a session key encrypted with a permanent key for the validation center.

10. The method of claim 9 wherein the authenticator is a data structure encrypted using the session key.

11. The method of claim 10 wherein the transmitting step (e) further comprises the substep of:

decrypting the ticket-granting ticket at the validation center to extract a session key.

12. The method of claim 11 wherein the permission data comprises an authenticator.

13. The method of claim 12 wherein the authenticator comprises a data structure encrypted with the session key.

14. The method of claim 1 further comprising the steps of:

transmitting a request for a server ticket from the network server to the validation center;

creating a server ticket for the network server at the validation center; and

receiving the server ticket from the validation center at the network server.

15. The method of claim 5 wherein the verifying step (f) further includes the substeps of:

extracting an access control list and verifying that the principal is authorized to access a digital certificate and a destination server key; and

issuing a digital certificate and a destination server key.

16. The method of claim 15 wherein the digital certificate conforms with the X.509 standard.

17. The method of claim 1 wherein the establishing step (g) further comprises the substep of:

establishing a secure connection from the network server to more than one destination server.

18. The method of claim 17 wherein each connection between the network server and a destination server is managed by a separate remote command execution client.

19. The method of claim 1 wherein the validation center utilizes a Kerberos protocol.

20. The method of claim 1 wherein the message comprises command data.

21. The method of claim 20 wherein the command data comprise a remote user name, a destination server list, and a command.

22. The method of claim 1 further comprising the step of temporarily storing the principal-authenticating information.

23. A method of providing a remote interactive login connection for a principal from a client computer through a network server to a destination server, comprising the steps of:

(a) obtaining credentials for authorizing the principal from a validation center;

(b) establishing a secure connection for exchanging data between the client and the network server;

(c) transmitting from the client computer to the network server the principal-authenticating credentials;

(d) transmitting the principal-authenticating credentials from the network server to the validation center;

(e) transmitting permission data for the network server from the validation center to the network server based on the principal-authenticating credentials;

(f) verifying the authorization of the principal in the network server to access a digital certificate and issuing a digital certificate to the network server;

(g) establishing a secure connection for exchanging data between the network server and the destination server based on the digital certificate; and

(h) executing a command interpreter in the destination computer

wherein the command interpreter may execute commands sent by the client computer.

24. A computer system for enhancing the security of one or more messages sent by a principal comprising:

a client computer for transmitting principal-authenticating credentials and the one or more messages;

a gateway computer operatively connected to the client computer, the gateway computer receiving principal-authenticating credentials and the one or more messages from the client computer;

a validation computer operatively connected to the gateway computer and capable of receiving the principal-authenticating credentials from the gateway computer and of transmitting permission data based on the principal-authenticating credentials to the gateway computer; and

one or more host computers operatively connected to the gateway computer and operating on any computer platform,

wherein, based on the permission data, the gateway computer establishes a secure connection with at least one of the one or more host computers, and

wherein the gateway computer transmits the one or more messages to at least one of the host computers.

25. The system of claim 24 wherein the gateway computer further comprises a gateway certificate server for transmitting the principal-authenticating credentials to the validation center and for receiving the permission data from the validation computer.

26. The system of claim 24 wherein the gateway computer further comprises one or more remote command execution clients for establishing one or more secure connections to the one or more host computers based on the permission data.

27. The system of claim 24 wherein each of the one or more host computers further comprises a host proxy and execution server for establishing a secure connection between each of the one or more host computers and the gateway computer.

28. The system of claim 27 wherein the host proxy and execution server executes a command interpreter for executing commands contained in the one or more messages.

29. A computer system for providing a remote interactive login connection comprising:

a client computer for transmitting principal-authenticating credentials;

a gateway computer operatively connected to the client computer, the gateway computer receiving principal-authenticating credentials;

a validation computer operatively connected to the gateway computer and capable of receiving the principal-authenticating credentials from the gateway computer and of transmitting permission data based on the principal-authenticating credentials to the gateway computer; and

one or more host computers operatively connected to the gateway computer and operating on any computer platform,

wherein, based on the permission data, the gateway computer establishes a secure connection with the host computer.

30. The system of claim 29 wherein the gateway computer further comprises a gateway proxy and execution server for establishing a secure connection to the at least one host computer based on the permission data

31. The system of claim 29 wherein the host computer further comprises a host proxy and execution server for establishing a secure connection between the at least one host computer and the gateway computer.

32. The system of claim 31 wherein the host proxy and execution server executes a command interpreter for executing commands.

33. The system of claim 29 wherein the client computer further comprises a downloadable executable interactive client (DEIC) for establishing a secure connection with the gateway computer.

34. The system of claim 33 wherein the downloadable executable interactive client (DEIC) comprises a Java applet.

35. The system of claim 29 wherein the gateway computer temporarily stores the principal-authenticating information.

36. A computer program product for use with a computer system,

the computer program product comprising a computer readable storage medium and a computer program stored therein for carrying out a process comprising:

(a) obtaining by the client computer credentials for authorizing the principal from a validation center;

(b) establishing a secure connection for exchanging data between a client and a network server;

(c) transmitting from the client computer to the network server the principal-authenticating credentials and the message;

(d) transmitting the principal-authenticating credentials from the network server to the validation center;

(e) transmitting permission data for the network server from the validation center to the network server based on the principal-authenticating credentials;

(f) verifying the authorization of the principal in the network server to access a digital certificate and issuing a digital certificate to the network server;

(g) establishing a secure connection for exchanging data between the network server and a destination server based on the digital certificate; and

(h) transmitting the message to the destination server.